STRATEGY RESEARCH PROJECT

CLOSE ACCESS INFORMATION OPERATIONS

BY

LIEUTENANT COLONEL JIM SLAVIN
United States Army

USAWC CLASS OF 2000

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Close Access Information Operations

by

LTC Jim Slavin
U.S. Army

COL James F. Powers, Jr.
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: LTC Jim Slavin

TITLE: Close Access Information Operations

FORMAT: Strategy Research Project

DATE: 10 April 2000 PAGES: 22 CLASSIFICATION: Unclassified

The information age comes with the challenge of implementing offensive information operations. As the United States executes the National Military Strategy, we must understand that our future threats may value information even more than we do. We have to further delineate responsibilities for conducting offensive information operations. With the technological security advances and reliance upon closed information systems, we must prepare an operational force that will be prepared to conduct close access offensive information operations. Finally, we must have the necessary intelligence collection for supporting such a force.

TABLE OF CONTENTS

CLOSE ACCESS INFORMATION OPERATIONS

The threats that the United States now faces are varied and multi-dimensional. In preparing to deal with each, whether a peer competitor or rogue state flaunting an asymmetrical threat, there exists a common vulnerability among each – **Information**. With the need for accurate and timely information, a potential adversary will take every possible means to secure this valued asset. The latest advances in technology are providing security measures that make it very difficult to attack their information from a distance. Therefore, the United States military must have a force ready to attack this vulnerability. As well, the Intelligence community must have the proper intelligence to support such operations.

This paper examines four main points in this approach. First the U.S. potential adversaries and their reliance upon information; second, the means for assuring information security; third the force of choice for close access operations; and finally our ability to support such valuable operations with the needed intelligence. Is the U.S. capable of dealing with the current doctrine of Offensive Information Operations?

NATIONAL MILITARY STRATEGY AND OFFENSIVE INFORATION OPERATIONS

The U.S. National Military Strategy is founded upon three elements: Shaping the International Environment, Responding to the Full Spectrum of Crises, and Preparing Now for an Uncertain Future.[1] To be an efficient and effective military force within these three elements, as well as across the entire spectrum of military operations, there exists a common thread that we need to find and then influence -a potential adversary's information. As defined in Joint Doctrine for Information Operations, "Information Operations (IO) involves actions taken to affect adversary information and information systems while defending ones own information and information systems."[2] While our defensive capabilities are very important, we must prepare to support the offensive capability in order to shape and respond in the information age. As well, it is important that we prepare a trained and ready force that can conduct offensive information operations that shapes today's environment or respond to tomorrow's uncertain crises.

THE VALUE OF INFORMATION

Why has information become so important? It has always been valuable to every nation and their ability to wage war. Napoleon espoused the view that "war is 90 percent information."[3] If this was true for his campaigns, I believe the importance has even increased with the onset of the information age. It has taken on such amplified emphasis for one major reason - the lethality and accuracy of today's weapon systems. With the expansion of technology, we are now able to generate and transfer information much quicker and in much greater volumes than ever before thus taking advantage of these weapon systems. If the information is correct, we can drop a 2000-pound bomb down a smokestack and disrupt an Iraqi command and control headquarters. If the information is incorrect, we end up bombing the Chinese embassy in downtown Belgrade.

Like the rest of the Defense Department, "The Army is embracing a new era characterized by the accelerating growth of information, information sources, and information dissemination capabilities supported by information technology. This new era, the so-called *Information Age*, offers unique opportunities as well as some formidable challenges."[4] As we move from the industrial to the information age, we rely upon timely and accurate information to expand today's weapons' effectiveness while trying to continually field the most advanced force with the proper doctrine.

Clausewitz noted that "each age has had its own peculiar forms of war."[5] We are progressing from the industrial age and we must be prepared to conduct total war in the information age. It is time we moved further with information operations (IO) and acquire the intelligence necessary to support it. We must have the ability to go beyond the indirect IO components, such as psychological operations, operations security (OPSEC) and deception. We should formulate unambiguous doctrine, establish a capability to conduct close access, offensive information operations, and have the intelligence assets available to support such maneuver against any potential adversary.

THE THREAT

In the days of the bipolar cold war, we were focused on the capabilities and intentions of the Soviet Union. We were confident that no matter what threat or disturbance arose, we could trace it back to and deal with the Soviet leadership for resolution. Based upon the decades of this single-mindedness, we were confident in the evolution of our doctrine, tactics, techniques and procedures. We not only confidently knew who the enemy was, but also more importantly, what and where his weaknesses were.

With the collapse of the Soviet Union, the entire paradigm has changed. As we no longer look in one direction for our threat, the ability to know a potential adversary is much more difficult. The latest risk assessments to our national well being can be categorized by four main themes: Lack of a Peer Competitor, Asymmetric Threats, Weapons of Mass Destruction, and Regional Threats.

General Hughes, former Director of the Defense Intelligence Agency (DIA), believed that a threat, such as the former Soviet Union would not be formidable for at least the next two decades.[6] "We are not confronted by a "peer competitor" – a hostile power of similar strength and capability – nor are we likely to be in the near future."[7] While this may be the prevailing thought regarding a peer competitor, there are a number of issues, such as nuclear weapon accountability that should cause us concern as the Russian leadership deals with both its economic and democratic development. Additionally China is developing "a military that can react quickly in the region with new precision weapons and modern combat platforms."[8] While today there may be no peer competitor, the economic and political situations of both Russia and China are still major reasons for concern and focus. As in the past, these countries will rely and secure the most accurate information available to prepare and conduct successful military operations. While these two countries may not be categorized as "peers", they are certainly significant and powerful enough to warrant constant notice. We must work diligently to know both their capabilities and intentions. If we can envision and affect their information systems, future confrontations would be greatly in our favor.

As characterized by DIA, the asymmetric threat will take advantage of an adversary's strengths while exploiting our perceived weaknesses.[9] The most likely threat would be that of terrorism. As Defense Secretary Cohen remarked, "Very little is needed other than knowledge and a computer and a modem. That is going to be less traceable to state-sponsored terrorism and you're going to have more potential for pranks. It could be the lone ranger who carries a grudge."[10] While we have prepared for terrorists in the past, this is certainly a different level of threat than we have faced before. It now requires us to better understand the breadth of such technological challenges. For example, the explosion of information availability via the World Wide Web has dramatically improved both access to and use of the world's information. It is not unrealistic to use the web's anonymity to carry out electronic hacking of even the Pentagon's systems. If a potential adversary would use offensive IO, we should be prepared with counter-offensive IO.

Third, DIA outlines in their support to the *National Security Strategy*, "Proliferation, particularly with regard to nuclear, chemical, and biological weapons and missile delivery systems, constitutes a direct threat to U.S. interests worldwide."[11] Additionally, Senator John Kerry, as chairman of the Senate Select Committee on Intelligence, was very concerned with the possibility of proliferation as nations sought to use their technical know-how for economic purposes. "If Libya, Iran, Iraq, or North Korea crash the nuclear club in coming years, it will be because the Chinese government has sold the country the components, materials and/or expertise to construct nuclear and/or chemical weapons."[12] No matter the supplier, China or Russia, the laws of the market economy are just as valid for nuclear proliferation as they are for selling oil. If the market will bare the cost, products will go to the highest bidder. It is readily apparent that there is a major reliance upon secure information to conduct such transactions as well as use the nuclear or chemical weapons. The U.S. Army Intelligence XXI Task Force states, "With the proliferation of WMD, our soldiers will face this threat everywhere in the world."[13] Proliferation will depend greatly upon the benefits of the information age as weapons, knowledge and finances use the advantages of technology.

The fourth major theme revolves around regional threats. As outlined in our *National Military Strategy*, "The potential for conflict among states and groups of states remains our most serious security challenge."[14] For centuries, this has been the case as cultures have clashed over ideas, land or even racial hatred. As outlined in the Army's Intel XXI case study, "We must be prepared to face rogue states capable of conventional military operations, especially against its neighbors."[15] The importance is that nation states, recognized or rogue, are relying upon the proliferation of information and will use it for their advantage as never before.

While I have categorized the likely national threats into four categories, Joint Doctrine for IO states, "It is difficult to predict which nation or groups may threaten our interests and how and when such threats will emerge."[16] The Army Intel XXI Task Force sums up the situation very skillfully, "One thing is certain, our foes will be learning and adaptive thanks to the Internet and the means to access it."[17]

As one looks across this spectrum of threats, what is the common denominator upon which we can focus for leverage? Because of the wide disparity in structure and motivation, each may have a variety of capabilities and limitations. However, based upon the expanses of technology, they share a common vulnerability – reliance upon accurate information. With advanced and inexpensive technologies, almost any country in the world has the capability to gain, access and transmit information in greater volumes and speed than ever before. Such information, coupled with technology based weapon systems, particularly, weapons of mass destruction, causes a great concern for our vital national interests. As countries and their weapon systems have become extremely information dependent, we should prepare a capability to use the information, rather than attacking the weapon system.

Once armed with our adversary's information, we have a number of choices. If it is to our advantage, we can do nothing. Secondly, we could react with any one of our capabilities, War or Military Operations Other Than War as outlined in our doctrine for Joint Operations. A final option would be to take his information, alter it, and affect his actions. In accordance with Joint Doctrine of Information Operations, this would be categorized as Offensive Information Operations.[18]

OFFENSIVE INFORMATION OPERATIONS

The need for an approach and prepared force for Offensive Information operations is clear from former Air Force Chief of Staff, Gen. Michael Dugan in his remarks to the Aerospace Education Foundation. "Just as classic Napoleonic maneuver tried to isolate an army from its logistics base, current strategies are looking for more and more ways to isolate warriors from crucial flows of information that provide or confront battlefield awareness."[19]

In Croatia, Offensive IO were as simple as alerting the Croatian Ministry of Defense knowledge concerning SA-6 RADAR. After our defense attaché presented facts to the Croatian government that we knew about all the facts concerning the radar, they decided to turn it off and move it.[20] While this act may not seem intriguing, the fact is that a hostile enemy system was made inoperable just by applying information. It was as simple as letting them know what we knew. They could then assume the consequences of our awareness.

Our joint doctrine asserts that, "Offensive IO apply perception management actions such as PSYOP, OPSEC and military deception, and *may* apply attack/destruction to produce a synergistic effect against the elements of an adversary's information systems."[21] We should release the conditional wording of *may* in doctrine. This would, without qualification, place offensive IO with other actions such as PSYOP, OPSEC, and deception. There would then be no doubt concerning our need for a trained and ready force supplied with the most advanced systems and intelligence. We would then have a clear direction for conducting attacks upon the information systems of adversaries. Next, a prepared force must be charged with the responsibility to conduct these operations.

Whether the focus of a potential adversary is in the potential peer category or the emerging group of nation states, there are two major enemy informational categories necessary to support military

operations: capabilities and intentions. While there are many categories of capabilities, (personnel; weapons; transportation; command, control and communications; etc.), this is just half the requirement. We must also know the intentions of the leadership. It is the intentions of the national and military leaders that will drive the use of their capabilities. To a degree, we have always had an ability to identify the enemy's capabilities and to some lesser degree his intentions, but we now must have the capability to directly affect the leaders ability to make decisions in conjunction with the indirect effects of psychological or deception operations.

In the fall of 1998, we were confident in our knowing the capabilities of the Iraqi armed forces as they moved South toward Kuwait. We knew their composition and disposition, right up to and through their invasion of Kuwait. However, we failed to know the intentions of Saddam Hussein. While he told us one thing, he was preparing for just the opposite. What would have been the outcome if we could have had a better read on his intentions and then affected his intentions through offensive IO?

James Adams in his novel, The Next World War, succinctly illustrates where the vulnerability lies. It is "to use adversaries information technology to get inside and disrupt an enemy's OODA (Orient, Observe, Decide, Act) loop; that is to enable yourself to make decisions faster and more efficiently while at the same time destroying the enemy's ability to make decisions."[22] It is the destruction, or manipulation of the enemy's ability to make decisions that is key. The process is to first know the intentions of the leadership and then be able to influence the operations. As stated in joint IO doctrine, "The human decision making processes are the ultimate target for offensive IO."[23]

Alvin and Heidi Toffler discussed the need for operations that would prevent war. They termed such operations as "anti-war". "Anti-wars, more important, include actions taken by politicians, and even warriors themselves, to create conditions that deter or limit the extent of war."[24] We have seen that both the politician and the soldier must be prepared for anti-war in the context of offensive information operations.

It is no surprise that as recently as the Kosovo campaign, President Clinton issued a "finding", authorizing the CIA to begin efforts "to find other ways to get Milosovic." One of the portions was for the CIA "to conduct a cyberrwar against Milosovic, using government hackers to tap into foreign banks." [25] Such intentions by the national command authorities illustrate the coming of age of the desire to and the need for offensive information operations.

Therefore, it is vital that we continue to not only know about the spectrum of potential enemies, but also have the capability to affect his decision making process. While entering into an enemy's OODA loop is not a trade secret, it must be a capability we come to the table with and be prepared to use all the tools available from our technology. It will certainly not be easy. With the value of knowledge being more valuable than ever before, all of our potential adversaries will do everything possible to secure their information as well as the means by which it is transmitted and stored.

ELECTRONIC SECURITY

With information as a major vulnerability, an enemy's ability to secure it has taken on global proportions over recent years. As George Tenet, Director of Central Intelligence, stated to the Senate Armed Services Committee hearing on current and projected national security threats, "Many of our targets are paying closer attention to information security, and many are adding emphasis and resources to deny and deceive our intelligence gathering capabilities."[26]

With immense expansion of security research and development on the business and economic fronts, military applications have and will continue to expand. Recent innovations range from security auditing services to vulnerability security reviews to systems that help reconfigure a network to be as secure as possible.[27]

With the OODA loop of the enemy as a key target, we must have the capability to access and affect his information. For such operations, some believe it can be achieved from afar via the Internet. Because of the Internet and its connectivity to the World Wide Web, the means would seem to be easy to enter into a country's database and take advantage of its accessibility. Internet hacking has emerged as a real threat to information assuredness. As witnessed on February 8, 2000, major commercial networks such as Yahoo, eBay and CNN were shut down due to, "an unprecedented campaign of electronic assaults against the biggest names in cyberspace."[28] However, it is not that simple. As these sites are in the business of being connected to the world for commercial purposes, they set themselves up for such attacks. It is not the same as an adversary's system that has been designed and built with maximum security in mind.

Even with multiple security systems and procedures within the US, commercial hacking, as well as military applications, have been increasing routinely. "In 1998, federal prosecutors opened 419 computer criminal cases, a 400 percent increase from 1992." [29] The Defense Department has been just as vulnerable. The Pentagon's mid-1997 "Eligible Receiver " exercise carried out by a team of about 30 computer specialists form NSA, showed the theoretical vulnerability of American civilian or military logistics and infrastructure to cyber-attack."[30] Whether it is the vulnerabilities highlighted by the Defense Department, or the recent commercial attacks, security needs cause various methods and technologies to be used in response to such actions. For example, in response to the hacker attacks of February 2000, security corporations immediately began to focus on improving methods for assuring the systems can be used without outside interference. These security actions will continue to proliferate as the need for commercial and military applications arise.

Security has many different aspects involving either software or hardware applications. The approaches for protection can range from obscurity, to host security, to securing the entire network.[31] Obscurity is based upon the assumption that no one knows the system exists.[32] Such a system would not be appropriate for major organizations, but this approach might work for an emerging threat or one with low visibility and high personnel security, such as a terrorist organization. The second method is defined as host security. This involves securing each machine separately. While again this would only

be practical for small-scale operations, the requirements for standard operating procedures necessitate many restrictions and many people to be effective.

The third method, network security, entails securing network access to various hosts and services.[33] What becomes evident is that as the organization expands, so does the need and complexity of the security system.

One very effective piece of network security is categorized as encryption. "Encryption is the transformation of data into a form that is as close to impossible as possible to read with out the appropriate knowledge (key)."[34] The more important the information, the more complex the encryption algorithm. For example, in today's commercial industry, "it has been said that one is safer using credit cards over the Internet than within a store or restaurant."[35] "Cryptography makes secure websites and electronic safe transmission possible."[36] Using encryption technology on a nation's most valued military information (capabilities and intentions) will deter access from distant locations. Knowing what the key is will require technical support for processing the algorithms or access to someone who has the keys.

Another valuable piece of network security is termed a firewall. "A firewall is a set of hardware components – a router, a host computer, or some combination of routers, computers and networks with appropriate software."[37] It serves network security by restricting entry and exits at a carefully controlled point and prevents attackers from getting close to the other defenses. Because all traffic passes through this point, the firewall assures that the traffic is acceptable.[38] Because of the barrier-like attributes, it requires access inside the firewall in order to alter the data. This requires close access.

We will therefore need to get a force inside the encryption and firewall. This force must not only know where and how to enter the system, but also be prepared for the spectrum of possible contingencies. It is likely that an adversary's important information systems would have the highest degrees of security. The challenges would range from passwords to firewalls, to active guard forces. The intelligence required certainly puts varied challenges upon the current collection capabilities of our intelligence community. Are we prepared?

FORCE OF CHOICE

In order to overcome the security challenges discussed above, it will take a force that can achieve close access and successfully conduct the technical and tactical challenges of IO. There appears to be two broad options for a force of choice – one would be local nationals and the other, military forces.

First, local national civilians have many advantages. The greatest is their familiarity within the region. By knowing the environment, they would be well suited for operating with anonymity. Their knowledge of the geography, population as well as customs and courtesies are strengths for operating in and around the information network. This advantage provides additional return. They may have a better chance for gaining admission to remote or restricted areas, a major advantage of close access operations. They can also blend into the environment if a deteriorating situation would arise.

The major disadvantages for a local national are recruiting, training, and gaining our trust. While the selection and training are achievable with the right person and sufficient time, formulating a sufficient level of trust is the high risk variable. For such highly sensitive operations, it would be difficult to put faith in any local national's ability to act for us. It is therefore advantageous to look to a military option for offensive IO.

The military option has gained steady momentum over the past several years. On October 7, 1999, Secretary of Defense Cohen announced changes to the Unified Command Plan. U.S. Space Command (USSPACECOM) is to become the lead military agency for computer network defense. It will also eventually be in charge of computer network attack.[39] These policy adjustments have not only added emphasis to our need for offensive IO, but also assigned responsibility to a Unified Combatant Commander.

While this would seem to put the entire responsibility within USSPACECOM, there is still a need for a military force that can implement the programs. General Myers, USCINCSPACE, did not envision his command as "the focal point where the keystrokes are made."[40] He stated that USSPACECOM would figure out the capabilities, focus, and test the work through the policy and legal implications.[41] This translates into staff responsibility. With the nuances of such operations, there will be numerous issues that USSPACECOM must address. However, we must assume that these administrative requirements will be satisfied and it will require an implementation force to conduct close access offensive information operations. The force of choice must be one that has the mission and the capability.

As outlined in Joint Doctrine for Special Operations, as well as 10 USC 164, 10 USC 167, IO are one of the eight activities designated as a principal special operations mission.[42] Our current doctrine is very specific that IO would involve actions to affect adversary information and information systems.[43] Our doctrine also states that "An adversary's nodes, links, human factors, weapon systems and data are particularly lucrative targets, capable of being affected through the use of lethal and non-lethal applications of coordinated SOF IO capabilities."[44] Within such parameters are many technical, tactical and many uncharted challenges. To affect these nodes it will take soldiers that are not only technically and tactfully proficient, but a force that is able to respond to various unforeseen circumstances.

The special operations soldier is well suited for such training and commitment. GEN Peter Schoomaker, Commander in Chief, U.S. Special Operations Command (USCINCSOC), summed up the abilities in his characterization of SOF. "We have mature people on the ground who speak the language and can access the situation and take action."[45] Under the category of strategic agility, SOF capability comes with a high degree of knowledge concerning the operational area because of routine and recurring training in foreign countries. Along with a specific geographic focus, SOF brings the necessary foreign language proficiency.[46]

The personnel that inhabit the SOF community, while armed with the latest technologies, realize that people are the most important asset. "It takes a discriminating selection and assessment process

and hard work to find the right person."[47] Because of this filtering process the SOF team must meet pre-designated, appropriate standards before entering the force. It takes such a philosophy to field a force that can operate in an environment with the technical and tactical challenges involved for close access IO.

Many of the technical challenges concerning IO can be met uniquely within the USSOCOM because its Title 10 authority to conduct research, testing and evaluation. This capability allows for timely actions in today's rapid technology expansion.[48] The inherent technical challenges for close access operations will certainly be better tackled because of this legislative advantage. But it will take more than technology. It will take a focused intelligence collection capability to overcome such innate challenges. These range from the usual characteristics of intelligence preparation of the battlefield relating to weather, enemy, and terrain to the technological security barriers of encryption and firewalls.

INTELLIGENCE SUPPORT

Due to such access challenges, a robust intelligence system must be in-place to support our efforts. Most important, the Intelligence Community (IC) must now be able to provide the technical characteristics that will allow access and intrusion to secured information and the means to alter the data, all without being discovered. Additionally, detailed intelligence must be provided concerning the environment in which the force must operate. Offensive IO present new and unique requirements now levied on the intelligence system resulting in a requirement for expanded collection. Without some realignment of resources, the current intelligence structure will not be able to support IO.

Based upon the assumption that the defense budget will not increase to any substantial degree, or that there will be a realignment of current appropriations, we must critically examine our defense expenditures so that areas that have the greatest effect will receive the highest priority. It is clear that our military lethality is well ahead of any international competitor. So why do we not put the priority where we will gain the most advantage? If the international community has learned anything through our experience in Desert Storm, the United States military arsenal can not be given time to prepare. Unless we greatly improve the effective use of our intelligence system, our reaction in using the instruments of national power may come too late. We can ill afford any major intelligence failures.

The IC, primarily through the use of Signals Intelligence (SIGINT), Photographic Intelligence (PHOTINT), and Human Intelligence (HUMINT), gains access to information throughout the world. With the state of our technological advances, SIGINT and PHOTINT are able to provide unmatched, timely and accurate information. While there are advances that continually need to be researched, the overall state of these two intelligence disciplines remains close behind spiraling technological advances. For years we have been very dedicated to put the majority of resources towards the technological solutions. While these two disciplines may provide a part of the picture, they do not tell the entire story.

To know a potential adversary's capabilities and intentions it requires more than the access provided by SIGINT and PHOTINT. This would not be a concern if our HUMINT readiness was at the

same state of preparedness as the other disciplines (SIGINT and PHOTINT), but it is not. Mr. Jack Downing, recently retired Deputy Director of Operations at the Central Intelligence Agency (CIA), expressed his concerns for the state of HUMINT access, "Over the next few years there still will be a paucity of trained personnel overseas."[49] The problem for HUMINT is very basic. It has been neglected over the past several years and it takes time to implement. First, it takes time to train personnel in both language and tradecraft skills. The language proficiency needed to operate within a foreign country may take up to two years to master. Additionally, the skills of the trade must be flawless and this can take another two to three years. Expert tradecraft is to ensure not only mission accomplishment, but also human survival. It then takes time to place that individual within the area of interest and then more time for this American to gain access to the information available.

Through the efforts of Mr. Downing and the IC, recruitment and training have been re-energized for HUMINT assets. Stated very well in the Washington Post, the estimates are that the spy force would increase in size by about 30 percent over the next seven years. According to this estimate, this would bring the force to approximately 1300 operations officers.[50]

As we have seen in the past several years, our top intelligence priorities are not where the emergencies occur. As an unfortunate example, I am confident that we would not find such HUMINT operations in either Tanzania or Kenya. If so, perhaps the embassy bombings could have been prevented. I submit that we can not wait the seven years. Additionally, these additional 1300 HUMINT operators will not be sufficient. We need to implement a policy immediately that will shore up this collection effort before the projected seven-year timeframe. We must reconsider where our trained HUMINT assets are currently assigned and revalidate the need in that particular country. We must reapportion these assets to the areas that are most likely to effect our vital national interests as well as those countries that provide the most beneficial access. As this 30 percent increase arrives within the next seven years, we can then realign to areas of the world with lesser US interests.

THE ROAD AHEAD

The threats that we are facing as we move into the information age, while seemingly disparate, all have the common vulnerability of information. Information Operations, though new and tagged with unique challenges, bring a contemporary dimension to the battlefield where we need to be prepared. While the U.S. military deals with the doctrinal and force planning challenges, the intelligence community must better prepare itself for supporting the needs of such acts with a robust human intelligence collection capability.

WORD COUNT = 5145

ENDNOTES

[1] John M. Shalikashvili, National Military Strategy of the United States of America. (Washington, D.C.: Joint Chiefs of Staff, 1997), 11.

[2] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13. (Washington, US Joint Chiefs of Staff, 9 October 1998), vii.

[3] Kreisher, Otto. "Nest Steps in Information Warfare," June 1999, Vol 82, No5; available from http://www.afa.org/magazine/0699nextstep.html; Internet accessed 3 February 2000.

[4] Department of the Army, Information Operations, Field Manual 100-6 (Washington, D.C.: U.S. Department of the Army,August 1996, iv.

[5] Alvin and Heidi Tofler, War and Anti-War. (New York: Warner Books, 1995), 95.

[6] Patrick M. Hughes, "A DIA Global Security Assessment." Defense Issues, vol. 12, no. 17, (1997): 1.

[7] Shalikashvili, 8.

[8] ROA National Security Report, 124.

[9] Hughes, 2.

[10] William Cohen, "Visions of Future Threats Facing the US," interview by Barbara Starr and Stacey Evers, Jane's Defence Weekly, 13 Aug 1997, 32.

[11] Hughes, 2.

[12] John Kerry, The New War (New York: Simon & Schuster, 1997). 56-57.

[13] Claudia J Kennedy, Army Intel XXI Task Force (Washington, D.C.: The Pentagon, June 1999), 1-5.

[14] Shalikashvili, 8.

[15] Kennedy, 1-5.

[16] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13. (Washington, D.C.: Joint Chiefs of Staff, 9 October 1998), I-1.

[17] Kennedy, 1-5.

[18] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13. (Washington, Joint Chiefs of Staff, 9 October 1998), I-5.

[19] Kreisher.

[20] James Adams, The Next World War (New York: Simon and Schuster, 1998), 89.

[21] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13. (Washington, Joint Chiefs of Staff, 9 October 1998), II-3.

[22] Adams, 108.

[23] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13. (Washington, D.C.: Joint Chiefs of Staff, 9 October 1998), II-1.

[24] Tofler, 3.

[25] Gregory L. Vistica, "Cyberwar and Sabotage." Newsweek, 31 May 1999, ?????

[26] George G. Tenet, "The Threat: An Intelligence Assessment," American Intelligence Journal, (Spring 1999): 13.

[27] "Penetration Testing," Information Security, (December 1999): 127 [database on-line]: available from Lexis-Nexis.

[28] Ted Bridis. "Buy.Com, eBay, Amazon, CNN Hacked: Assaults Similar to One That Overwhelmed Yahoo!" 9 February 2000.

[29] Tom Guarisco, "Web Security: Threat of Hacking Growing with e-commerce," 30 January 2000; available fromhttp://www.theadvocate.com/business/story.asp?storyID=1808; Internet, accessed 31 January 2000.

[30] Bob Drogin. "In Theory, Reality, U.S. Open to Cyber-Attack: Security : A NSA Test Exposed Vulnerability of Critical Computer Systems to Hackers. Outside Assault Proved It, " Los Angeles Times, 9 October 1999, part A, 19.

[31] D. Brent Chapman and Elizabeth D. Zwicky, Building Internet Firewalls (Sebastopol, CA: O'Reilly & Associates, Inc., 1995), 13-16.

[32] Ibid., 13.

[33] Ibid., 15.

[34] RSA Laboratories, FAQ 4.0 (n.p.), 10.

[35] Ibid., 16.

[36] Ibid.

[37] Chapman, 17.

[38] Ibid.

[39] Grier, Peter, This Month in Aerospace World:UCP Changes, Space Command to Guard the Networks," December 1999, vol. 82, no. 12; avail from http:///www.afa.org/magazine/world/1299world.html; Internet; accessed 3 February 2000.

[40] Ibid.

[41] "Special Defense Department Briefing: Current Activities of the U.S. Space Command," (5 January 2000): [data base online]; available from Lexis-Nexis.

[42] Joint Chiefs of Staff. Doctrine for Joint Special Operations. Joint Publication 3-05. (Washington, D.C.: Joint Chiefs of Staff, 17 April 1998), II-2.

[43] Joint Chiefs of Staff. Doctrine for Joint Special Operations. Joint Publication 3-05. (Washington, D.C.: Joint Chiefs of Staff, 17 April 1998), II-10.

[44] Joint Chiefs of Staff. Doctrine for Joint Special Operations. Joint Publication 3-05. (Washington, D.C.: Joint Chiefs of Staff, 17 April 1998), II-11.

[45] Glenn W. Goodman, "Global Scouts with a Ubiquitous Presence," Armed Forces Journal International (February 1999): 48.

[46] Goodman, 46.

[47] Special Operations Command, United States Special Operations Posture Statement , (Tampa, FL, 1998), 14.

[48] US Code. Title 10, Chapter 6, Sec. 167.

[49] Walter Pincus, "Top Spy Retiring from CIA; Downing Lead Revamp Of Clandestine Service," The Washington Post, 29 July 1999, sec. A, p.27.

[50] Vernon Loeb, "At Hush-Hush CIA Unit, Talk of a Turnoaround; Reforms Recharge Espionage Service," The Washington Post, 7 September 1999, sec. A, p. 8.

BIBLIOGRAPHY

Adams, James. The Next World War. New York: Simon and Schuster, 1998.

Bridis, Ted. "Buy.Com, eBay, Amazon, CNN Hacked: Assaults Similar to One That Overwhelmed Yahoo!", February 9, 2000.

Chapman, D. Brent, and Elizabeth D. Zwicky. Building Internet Firewalls. Sebastopol, CA: O'Reilly & Associates, Inc., 1995.

Cohen, William. "Visions of Future Threats Facing the US," Interview by Barbara Starr and Stacey Evers. Jane's Defence Weekly, 13 Aug 1997, 32.

Clinton, William J. A National Security Strategy for a New Century . Washington, D.C.: The White House, October 1998.

Coffman, David W. "Operational Art and the Human Dimension of Warfare in the 21st Century." Essays 1999 (1999): 67-95.

Commander, Joint Warfighting Center. Concept for Future Joint Operations Ft Monroe, VA.:Joint Wasrfighting Center, May 1997.

Drogin, Bob "In Theory, Reality, U.S. Open to Cyber-Attack: Security : A NSA Test Exposed Vulnerability of Critical Computer Systems to Hackers. Outside Assault Proved It." Los Angeles Times, 9 October 1999, part A, p.19.

Goodman, Glenn W. "Global Scouts with a Ubiquitous Presence." Armed Forces Journal International (February 1999): 46-48.

Grier, Peter. "UCP Changes, Space Command to Guard the Networks." December 1999. Available from http://www.afa.org/magazine/world/1299world.html. Internet. Accessed 3 February 2000.

Guarisco,Tom. "Web Security: Threat of Hacking Growing with e-commerce," 30 January 2000. Available fromhttp://www.theadvocate.com/business/story.asp?storyID=1808. Internet, Accessed 31 January 2000.

Hughes, Patrick M. "A DIA Global Security Assessment." Defense Issues, vol. 12, no. 17, (1997): 1-8.

Kerry, John. The New War. New York: Simon & Schuster, 1997.

Kennedy, Claudia J. Army Intel XXI Task Force. Washington, D.C.: The Pentagon, June 1999.

Kreisher, Otto. "Next Steps in Information Warfare," June 1999. Available from http://www.afa.org/magazine/0699nextstep.html. Internet. Accessed 3 February 2000.

Loeb, Vernon. "At Hush-Hush CIA Unit, Talk of a Turnaround; Reforms recharge Espionage Service." The Washington Post, 7 September 1999, sec. A, p.08.

Pincus, Walter. "Prescriptions for Keeping Secrets; Report on Chinese Espionage Inspires a Variety of Hill Proposals." The Washington Post, 29 July 1999, sec A, p.3.

Pincus, Walter. "Top Spy Retiring from CIA; Downing Lead Revamp of Clandestine Service." The Washington Post, 27 May 1999, sec A, p.27.

RSA Laboratories. FAQ 4.0 (n.p.) 1998.

Shalikashvili, John M. National Military Strategy of the United States of America. Washington, D.C.: Joint Chiefs of Staff, 1997.

"Special Defense Department Briefing: Current Activities of the U.S. Space Command." (January 5, 2000): Database on-line. Available from Lexis-Nexis.

"Stallings, William. Cryptography and Network Security: Principles and Practice. Upper Saddle River, New Jersey: Prentice-Hall, 1998.

Steele, Robert David. "The Asymetric Threat: Listening to the Debate." Joint Force Quarterly (Autumn/Winter 1998-99): 78-84.

Vistica, Gregory L. "Cyberwar and Sabotage." Newsweek, 31 May 1999, p. 38.

Tenet, George G. "The Threat: An Intelligence Assessment." American Intelligence Journal, (Spring 1999): 5-13.

Toffler, Alvin, and Heidi. War and Anti-War. New York: Warner Books, 1995.

U.S. Code. Title 10, Chapter 6, Sec. 167.

U.S. Department of the Army, Information Operations, Field Manual 100-6. Washington, D.C.: U.S. Department of the Army, August 1996.

U.S. Joint Chiefs of Staff. Doctrine for Joint Operations. Joint Publication 3-0. Washington, D.C.:U.S. Joint Chiefs of Staff, 1 February 1995.

U.S. Joint Chiefs of Staff. Doctrine for Joint Special Operations. Joint Publication 3-05. Washington, U.S. Joint Chiefs of Staff, 17 April 1998.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington, U.S. Joint Chiefs of Staff, 9 October 1998.

U.S. Special Operations Command, Special Operations in Peace and War. USSOCOM PUB 1. Tampa, FL.: United States Special Operations Command, 25 January 1996.

U.S. Special Operations Command, United States Special Operations Forces Posture Statement. . Tampa, FL.: United States Special Operations Command, 1996.